

UNITED STATES DISTRICT COURT

FILED

for the

Eastern District of North Carolina

JAN 14 2022

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY SG DEP CLK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)KIK ACCOUNT: "cshellston" STORED AT PREMISES
CONTROLLED BY KIK / MEDIA LABSCase No. 7:22-mj-1013-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

KIK ACCOUNT: "cshellston" STORED AT PREMISES CONTROLLED BY KIK / MEDIA LABS, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2251(a) and 2252A(a)(2)(A), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2251(a)	Production of Child Pornography
18 USC 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kelly Kucala
Applicant's signature

Kelly Kucala, Special Agent FBI

Printed name and title

Sworn to in accordance with Fed. R. Crim. P. 4.1 the applicant having appeared before me via reliable electronic means and under oath and attesting to the contents of this application.

Date: January 14 2022

Robert B. Jones, Jr.
Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr., U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
KIK ACCOUNT:
"cshellston"
STORED AT PREMISES CONTROLLED
BY KIK / MEDIA LABS

Case No.:

7:22-mj-1013-RJ

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kelly Kucala, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since January 17, 2021 and am currently assigned to FBI's Charlotte Division, Wilmington Resident Agency. I have received training and I have experience in federal law enforcement investigations. I have participated in the execution of search and arrest warrants. Additionally, I have conducted surveillance of the investigation's subject and the target location. As a federal law enforcement officer, I am charged with the duty of investigating violations of United States Code and collecting evidence in matters in which the United States is or may be a party of interest. I am charged with investigating a range of crimes, including human trafficking, violent crimes, and violent crimes against children including 18 U.S. Code 2251 Sexual Exploitation of Children and 18 U.S. Code 2552 Certain Activities Relating to Material Constituting or Containing Child Pornography. As a Federal Agent, I am authorized by the Attorney General to investigate violations of federal law of the United States and am a law enforcement officer with authority to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (the “**Target Accounts**”) that is stored at premises owned, maintained, controlled, or operated by MediaLab, Inc:

- cshellston

The Target Accounts are stored at premises owned, maintained, controlled, or operated by Kik Media Labs, a social media company headquartered at 1237 7th St., Santa Monica, CA 90401. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Media Labs to disclose to the government records and other information in its possession, pertaining to the subscriber(s) or customer(s) associated with the Target Accounts.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of U.S. laws will be located in the Kik Media Labs records described above.

4. The application for a search warrant, which this affidavit is offered in support thereof, is being applied for to seize instrumentalities, fruits and evidence more particularly described in Attachment B, of violations of 18 U.S.C. § 2251(a) (production of child pornography), 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of child pornography).

5. In summary, this affidavit set forth facts establishing probable cause to believe that within the Target Accounts there are instrumentalities, fruits and evidence of a subject who

manufactured received, distributed, and/or possessed via the Internet, images depicting minors engaging in sexually explicit conduct.

II. JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a “district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

III. RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), (b)(1); and 2252A(a)(5)(B), (b)(2) (collectively, “Specified Federal Offenses”).

8. Title 18 U.S.C. Section 2251(a) prohibits a person from employing, using, persuading, inducing, enticing or coercing any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

9. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or

conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

IV. DEFINITIONS

11. Based on my training and experience, as well as my consultation with other law enforcement officers, I understand that the following definitions and explanations apply to the activity discussed in the affidavit.

12. "Internet Crimes Against Children (ICAC) Task Force Program" is a task force Program (also known simply as ICAC) is a national network of sixty-one coordinated forces representing 4500 federal, state, and local law enforcement, and prosecutorial agencies. These agencies are continually engaged in proactive and reactive investigations and prosecutions of person involved in child abuse and exploitation involving the Internet.

13. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

14. "Visual depictions" include undeveloped film and videotape and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

15. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

16. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

17. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

18. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

19. The term "GUID", as used herein refers to the Globally Unique Identifier (GUID) identification number that may be issued by the Peer-to-Peer (P2P) software to computers offering

to share files on the P2P network. A GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

20. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of ["www.usdoj.gov"](http://www.usdoj.gov) refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

21. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific

information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

22. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

23. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

24. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that describes the specific location of a file in that computer.

25. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records; painting, typing) or electrical, electronic or magnetic form (including but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices,

portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

26. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

27. Based on my training and experience, I will use the following technical terms to convey the following meanings:

- a. *Cellular telephone*: A cellular telephone (or cellular phone or smartphone or mobile telephone, or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/ receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. *Cloud-based storage service*: as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need

to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

- c. *Computer*: The term “computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.
- d. *Computer Hardware*: The term “computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- e. *Computer Passwords and Data Security Devices*: The term “computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- f. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. *Computer Software*: The term “computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- h. *Electronic Communication Service ("ESP")*: as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.
- i. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.
- j. *File Transfer Protocol ("FTP")*: as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- k. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. *Internet Connection*: The term "Internet connection" means a connection required for access to the Internet. The connection would generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.
- m. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- n. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually

include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- o. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- p. *Remote Computing Service ("RCS")*: as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- q. *Short Message Service ("SMS")*: as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- r. *SIM card*: A Subscriber Identity Module, or SIM, is an [integrated circuit](#) chip, or electronic storage device, that is intended to [securely](#) store the [international mobile subscriber identity](#) (IMSI) number and its related [key](#), which are used to identify and authenticate subscribers on [mobile telephone](#) devices (such as [mobile phones](#) and [computers](#)). It is also possible to store contacts on many SIM cards. A SIM card contains its unique serial number ([ICCID](#)), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a [personal identification number](#) (PIN) for ordinary use, and a [personal unblocking code](#) (PUK) for PIN unlocking.
- s. *Storage Medium*: The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- t. *Wireless Network*: The term "wireless network" means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency.

Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

28. Based on my training, experience, and research, examining data stored on the data storage devices or network can uncover, among other things, evidence that reveals or suggests who possessed or used the account.

V. PROBABLE CAUSE

29. On Tuesday, November 16, 2021, the Federal Bureau of Investigation (FBI) Washington Field Office (WFO) received information that a Kik user, “cshellston,” display name “Craig Shellston,” was on a Kik group known for discussing and trading original images and videos of underage children. “Cshellston,” stated he was slightly sexually active with a seven-year-old female and that he would play with when she slept. “Cshellston” reported he would use Xanax to put the child into a deep sleep during the assault.

30. “Cshellston” verified himself on Kik by sending a picture of the seven-year-old victim sitting on the sofa, a picture of himself with the seven-year-old victim in the background, and a picture of himself holding up three fingers with the seven-year-old in the background. He then distributed child sexual abuse material (CSAM) he produced with the seven-year-old female seen in the verification photos.

31. The first video file, 64c1d8ea-f29-4f14-bd88-85adc7c7710, is 14 seconds in length and was sent from “chellston” at 6:46pm on November 16, 2021. In this video, the person controlling the camera placed an adult male erect penis on the victim’s lips.

32. The second video file, 460df9b1-ba88-48b1-8db0-c739806ad616, is 14 seconds in length and was sent from “chellston” at 7:37pm on November 16, 2021. In this video, the person controlling the camera placed an adult male erect penis on the victim’s lips.

33. The third video file, 4079204d-08b4-48c49cf2-971b89e5fbc0, is 12 seconds in length and was sent from “chellston” at 7:37pm on November 16, 2021. In this video, the person controlling the camera placed an adult male erect penis on the victim’s lips.

34. The fourth video file, Ac646e04-4af5-4c7b-9527-a6ef78d7149b, is 14 seconds in length and was sent from “chellston” at 6:46pm on November 16, 2021. In this video, an adult left hand, with black plastic bracelets and metallic ring on their left ring finger, removed a blanket to show a prepubescent female. The male moved the prepubescent female’s underwear to show her bare vagina. White sheets with avocado print were observed in the video.

35. The fifth video file, C89adf37-9ad4-4fd7-98e4-6f9fefce795e, is 14 seconds in length and sent from “chellston” at 6:46pm on November 16, 2021. This video depicted an adult left hand with black plastic bracelets and metallic wring on their left ring finger moving a prepubescent female’s underwear to show her bare vagina. The male hands then inserts his index and middle fingers into the bare vagina to spread and display the vagina. White sheets with avocado print were observed in the video.

36. Through an emergency disclosure form, submitted to Kik c/o MediaLab regarding the user “cshellston,” an IP address was identified, 98.24.229.122. The subscriber of this address was Rosemary Strawn, with a service address of 211 Cypress Bay Drive, Jacksonville, NC 28546, contact number 252-259-0404.

37. With this information, FBI Washington was able to fully identify the suspected user of Kik account “cshellston,” as William Austin Strawn, date of birth (DOB) May 12, 1992.

Strawn resided at 211 Cypress Bay Drive, Jacksonville, North Carolina and is married to Rosemary Strawn. Strawn's driver's license photograph appeared to the same individual in the pictures shared on Kik for verification.

38. This information was passed to FBI Wilmington Residency Agency. FBI Wilmington contacted Jacksonville Police Department and on Tuesday, November 16, 2021, William Strawn was arrested from his residence, 211 Cypress Bay Drive without incident. Jacksonville Police Department charged STRAWN in North Carolina with first degree sexual exploitation of a minor, second degree sexual exploitation of a minor, indecent liberties with a minor, and indecent exposure. Additional charges were added including child sexual exploitation material and statutory sex offense.

39. On Wednesday, November 17, 2021, during a post-arrest interview, STRAWN admitted to using the phone application Kik, where he went by the name "Craig Shellston." On Kik and Reddit, STRAWN admitted to exploring his "sexually perverse fantasies." STRAWN stated he would receive material he identified as "illegal," including sexually explicit videos of minors between the ages of five to ten years old. STRAWN reported he had last received this type of material Tuesday, November 16, 2021.

40. During the post arrest interview, STRAWN admitted he committed sexual acts with the seven-year-old victim but did not want to disclose them specifically. He admitted he shared pictures of himself and the victim on Kik and would verify himself but holding up a certain number of fingers in pictures.

41. Following the arrest, a state search warrant was executed on STRAWN's residence, 211 Cypress Bay Drive, Jacksonville, NC 2546. At the residence, avocado bedsheets were recovered. These bedsheets can be seen in the video shared over Kik, in which the victim

was being sexually assaulted. The living room appeared to be the location of the verification photographs sent over Kik with STRAWN and the victim pictured.

42. On Friday, November 19, 2021, the victim was interviewed at One Place in Jacksonville, NC. During the interview, the victim reported one night she woke up and saw STRAWN sitting on the bed where she was sleeping with his cell phone.

43. On Friday, November 19, 2021 at 6:07 pm, during a jail call between STRAWN and his wife, Rosemary, STRAWN admitted, "I did some fucking weird shit," with the victim. In addition, STRAWN states he would record himself masturbating while the victim slept, he would place his penis on the victim's face, and he took a dildo and placed it on the victim. STRAWN denied being attracted to children but said his actions had to do with "power."

VI. BACKGROUND REGARDING KIK MEDIA LABS CORP

44. The following information has been provided to me from the Kik Law Enforcement Guide (dated February 26, 2020), online research that I have conducted, from other law enforcement officers, as well as my training and experience. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cellphone. Kik advertised itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to its company website was designed to "break down barriers [between operating systems] that would allow users to chat with whoever, whenever." In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc. MediaLab Inc. is a holding company that owns other internet-based communication applications such as Whisper, Datpiff and others.

45. Kik Messenger is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user selects while still within the Kik platform. Unlike other messaging apps, Kik usernames - not phone numbers - are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters. A Kik username is the only publicly available identifier MediaLab Inc. can use to identify a Kik account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address.

46. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture-themed ideas as well as illicit/illegal-themed ideas. Public groups names are a user-generated hashtag; can never be replicated; can never be changed; may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters; The group hashtag will begin with a hash (#) (i.e. #AffidavitForWarrant).

47. Kik advises that upon service of an appropriate legal order, the company can provide the following non-content user data - Current first and last name and email address; Link to the most current profile picture or background photo; Device related information; Account

creation date and Kik version; Birthdate and email address used to register the account (new registrations after November. 2014); User location information, including IP address(es)[1].

KIK further advises that upon service of a search warrant, the company can provide the following content user data: Transactional chat log - Log of all the messages that a user has sent and received, including sender username, receiver username/receiver group JID[2], timestamps, IP of the sender and word count. This log does not include the actual message that was sent. If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames; Chat Platform Log - Log all the media files that a user has sent and received, including sender username, receiver username/receiver group JID, timestamps, IP of the sender, media type, and Content ID. If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames; Photographs and/or videos - Media files sent or received by the user for the last 30 days; Roster log - Log of usernames added and blocked by the subject user, including timestamps; Abuse reports - Transcript of reported chat history against the subject user, including sender username, receiver username, timestamps, actual message, and content IDs; Email events - Log of all the emails that have been associated with a username; Registration IP - IP address associated to the username when the account was registered, including timestamp. Additionally, the company advises that upon service of a search warrant, the company can provide the following content group data: Group information log - Current information about the group, including the group JID, group name(s), group type, and the status of the group; Group create log - Includes details about who created the group and at what time; Group join logs - A record of the users who have joined the group, including timestamps and the method that was used to join a group; Group leave logs - A record of the users who have left the group, including timestamps and the method that was used

to leave the group; Group transactional chat log - Log of all the messages that a group has received, including sender username, timestamps, IP of the sender, receiver username(s), and word count. This log does not include the actual message that was sent; Group chat platform log - Log of all the media files that a group has received, including sender username, timestamps, IPs of the sender, receiver username(s), media type, and content ID; Photographs and/or videos - Media files received by the group; Group abuse reports - Transcript of reported chat history against the subject group, including sender username, receiver username, timestamps, actual message, and content IDs. Kik Media Labs is considered an electronic communications service (ECS) provider because it provides its users access to electronic communications services as defined in 18 U.S.C. §§ 2510(15). Section 2703 of Title 18 of the United States Code sets out particular requirements that the government must meet in order to obtain access or disclosure of records communications, and other information from an ECS provider, and through this warrant, the government seeks such disclosures and the items identified in Attachment B.

VII. LOCATION TO BE SEARCHED

50. The Target Accounts are stored at premises owned, maintained, controlled, or operated by Kik Media a company headquartered in San Mateo, California located at 1237 7th St., Santa Monica, CA 90401. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Kik Media Labs to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

VIII. CONCLUSION

51. Your Affiant respectfully asserts that based on these facts, there is probable cause to believe that within the information associated with the Target Accounts, located at the facilities in the possession, custody and control of Kik Media Labs, there are presently files either active or deleted, created, accessed, modified, uploaded, downloaded or otherwise related to the Kik Media Labs account, which constitute evidence of the violation of the Specified Federal Offenses.

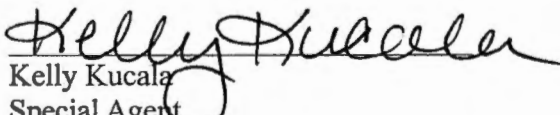
52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Kik Media Labs. Because the warrant will be served on Kik Media Labs, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

53. Wherefore, your Affiant requests authority to search the account described in Attachment A in order to seize items described in Attachment B in accordance with Rule 41 of the Federal Rules of Criminal Procedure, pursuant to Title 18 U.S.C. § 2703.

[Remainder of page intentionally left blank]

54. Your Affiant also respectfully requests that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further Order of the Court. This investigation is currently ongoing and the details in this Affidavit, if disclosed prior to the completion of the investigation, could compromise future undercover operations and alert the subjects, both known and unknown, to the existence of the investigation.

55. I declare under penalty of perjury that the foregoing information surrounding the request for a search warrant regarding the Target Accounts is true and correct to the best of my knowledge.


Kelly Kucala
Special Agent
Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this affidavit this 14 day of January 2022.


ROBERT B. JONES, JR.
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Kik Media Labs accounts (the “Target Accounts”):

- cshellston

The Target Accounts are stored at premises owned, maintained, controlled, or operated by KIK MEDIA LABS Corp a company headquartered in San Mateo, California located at 1237 7th St., Santa Monica, CA 90401

ATTACHMENT B

Particular Things to be Seized

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by MediaLab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab, Inc is required to disclose the following information to the government for each account or identifier listed in Attachment A:

All subscriber/account information and content related to the following Kik account:

Username: cshellston

Associated email address: craigshellston@gmail.com

1. Subscriber data, unrestricted by date, associated to the Kik account
 - a. Basic current subscriber information provided by the user, such as current first and last name and email address
 - b. Link to the most current profile picture
 - c. Device related information
 - d. Account creation date and Kik version
 - e. Birthdate and email address used to register the account
 - f. User location information
2. IP addresses associated to the Kik account from 1/1/2021 to present, including remote port information
3. All transactional chat logs associated to the Kik account from 1/1/2021 to present
4. All images and videos associated to the Kik account, including the unknown usernames and IP address associated to the sender of the images and videos from 1/1/2021 to present
5. A date-stamped log showing the usernames that the Kik account added and/or blocked from 1/1/2021 to present
6. All abuse reports associated to the Kik account, including the unknown usernames from 1/1/2021 to present
7. All emails associated to the Kik account from 1/1/2021 to present

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2251(a) - the sexual exploitation and attempted sexual exploitation of children, 18 U.S.C. § 2252A(a)(2) - distribution or receipt of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography involving the user of Kik account **cshellston** since 1/1/2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (d) Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
- (e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (f) The identity of the person(s) who communicated with the user ID about matters relating to sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.